**IN THE UNITED STATES DISTRICT COURT**
**FOR THE WESTERN DISTRICT OF MICHIGAN**
**SOUTHERN DIVISION**

| | |
|---|---|
| RYAN MILLIRON,<br>*Plaintiff*,<br><br>v.<br><br>UNITED STATES DEPARTMENT OF DEFENSE,<br>*Defendant*. | Civil Action No. 1:23-cv-1222<br><br>Hon. Robert J. Jonker<br>U.S. District Judge<br><br>Hon. Phillip J. Green<br>U.S. Magistrate Judge |

**MEMORANDUM IN SUPPORT OF DEFENDANT'S**
**MOTION FOR SUMMARY JUDGMENT**

## TABLE OF CONTENTS

## INTRODUCTION

Plaintiff Ryan Milliron filed this Freedom of Information Act ("FOIA") lawsuit to obtain from Defendant Department of Defense ("DOD") a single record, a report produced by a research laboratory at Georgia Institute of Technology ("Georgia Tech") and submitted to the Defense Advanced Research Projects Agency ("DARPA") as a proof of concept. The report, which analyzes and attributes a particular cyber-attack, is shot through with descriptions of the laboratory's research methods and the technology on which it relies to attribute cyber-attacks. After initially withholding the record in full, DOD, DARPA's parent agency, reprocessed the record and released it with redactions under FOIA Exemptions 4, 6, 7(C), and 7(E).

DOD's redactions were proper. Exemption 4 permits an agency to withhold "confidential commercial information" submitted to the agency by a non-governmental entity where disclosure of that information would cause harm. Those requirements are met here: Georgia Tech submitted information—closely held details about the statistical features of its proprietary algorithm and data sources on which that algorithm relies to function—that the university explicitly marked as confidential, under circumstances in which the university could reasonably anticipate that the agency would maintain that confidentiality. The information about statistical features and data sources is commercial, both because it inherently relates to commercial aspects of the technology (which Georgia Tech has licensed and for the use of which it receives royalties) and because its disclosure would have adverse implications for the commercial value of the algorithm. And relatedly, disclosure of the information would cause harm in one or both of two ways: competitive harm to Georgia Tech, and/or direct diminution in the value of its product. The Court should therefore grant summary judgment to Defendant on the propriety of its Exemption 4 redactions.

The redactions DOD made pursuant to Exemptions 6, 7(C), and 7(E) entirely underlie those made under Exemption 4, and so the Court need not address the latter three exemptions if it upholds Defendant's assertion of Exemption 4. In the event it does reach the issues, DOD's invocation of those three exemptions is also justified. As an initial matter, the record was compiled (by DOD) for law-enforcement purposes related to DARPA's research mission. As such, the personally identifiable information it contains, and the details it would provide foreign adversaries about the DARPA's investigative techniques (through reliance on Georgia Tech and other partners), trigger interests protected by Exemptions 7(C) and 7(E) respectively. By the mere fact that DOD possesses the record, the third-party personal information it contains also triggers Exemption 6. And these interests merit withholding the information. As for the third-party personal information subject to 6 and 7(C), there is no cognizable public interest in disclosure, because the information would not shed light on federal government activity. And disclosure of the information would infringe on those privacy interests (and lead to follow-on harms), much like the disclosure of the 7(E) information would weaken DARPA's ability to investigate malicious activity online.

The Court should grant summary judgment to Defendant.

## BACKGROUND

### I. DARPA's Enhanced Attribution Program and the Georgia Tech Report

DARPA, as a research component of DOD, "conducts and funds projects to enhance the capabilities of the U.S. military." Declaration of Joseph Whited ¶¶ 15-16, Ex. 1 ("Whited Decl."). One of DARPA's research programs, now concluded, was the "Enhanced Attribution" program. *Id.* ¶ 17. Observing that "[m]alicious actors in cyberspace . . . operate with little fear of being caught due to the fact that it is extremely difficult, in some cases perhaps even impossible, to reliably and confidently attribute actions in cyberspace to individuals," *see* DARPA, Enhanced

Attribution, https://perma.cc/U9SH-SBEP ("EA Website"), the agency undertook through the Enhanced Attribution program to "make currently opaque malicious cyber adversary actions and individual cyber operator attribution transparent by providing high-fidelity visibility into all aspects of malicious cyber operator actions and to increase the government's ability to publicly reveal the actions of individual malicious cyber operators without damaging sources and methods." EA Website. Specifically, the Enhanced Attribution program sought to "develop techniques and tools for generating operationally and tactically relevant information about multiple concurrent independent malicious cyber campaigns, each involving several operators, and the means to share such information with any of a number of interested parties." EA Website.

With the intention of participating in the Enhanced Attribution program, Astrolavos Lab, a laboratory at Georgia Tech, submitted a "proof of concept" report to DARPA in August 2016 in which it conducted in-depth analysis of the July 2016 cyber-attack campaign waged by Fancy Bear, a Russian cyber espionage group also known as APT28. Whited Decl. ¶¶ 3, 11-12, 19; *see generally* Record, Ex. 2. Fancy Bear's July 2016 campaign included a widely publicized intrusion into the email servers used by the Democratic National Committee. *See* David E. Sanger & Nicole Perlroth, *As Democrats Gather, a Russian Subplot Raises Intrigue*, N.Y. TIMES (July 24, 2016), https://www.nytimes.com/2016/07/25/us/politics/donald-trump-russia-emails.html. The report begins by noting that the "Fancy Bear/APT28 campaign, a cyber-interference campaign "apparently related to the recent cyber attack on the Democratic National Committee," "is widely attributed to Russian national efforts." Record at 2 (PDF pagination). Then, "combin[ing] machine learning techniques, large data analysis, and innovative feature selection," *id.*, the report describes and analyzes features of the cyber-attack (and the campaign more generally) with the goal of attributing responsibility for it, *see generally id.*

To produce the report, Astrolavos Lab relied on proprietary technology encompassed within the term the "Rhamnousia Framework." *See* Record at 2 (describing the laboratory's project as "combin[ing] machine learning techniques, large data analysis, and innovative feature selection). The framework is a proprietary research method that integrates algorithms to attribute cyber intrusions. Whited Decl. ¶ 18. By way of analogy, the technology at issue is "akin to a combination of a recipe and a roadmap: the recipe combines various sources of data to yield a technology product, which researchers use like a roadmap to find the source of a particular cyber-attack." *Id.* The continued reliability and success of the technology relies on both (1) particular public data sources and (2) Georgia Tech's attention to certain "statistical features" of cyber attacks that enable it to attribute those attacks. *Id.* Although developed in a university setting, the technology is commercially valuable—indeed, Georgia Tech, the ultimate owner of the technology, has licensed its use to a commercial enterprise, Voreas Laboratories, in exchange for consideration. *Id.* ¶ 24.

The distinctive features of the Rhamnousia Framework are on display throughout the report at issue in this litigation. Pages 3 through 18 of the report contain the report's analysis, in which its authors detail the features of the cyber-attack campaign they analyzed and their findings and recommendations. Whited Decl. ¶ 20; Record at 3-18. Numerous charts and graphs appear in the report, translating into visual form the statistical features and data sources on which the technology relies. Whited Decl. ¶ 20; Record at 3-18. The concluding pages of the report detail recommendations for further research, which themselves contain and highlight features the researchers found to be meaningful. Whited Decl. ¶ 20; Record at 18-19. And the second half of the 40-page document (pages 21 through 40) consists of its appendices, in which the authors detail their sources. Whited Decl. ¶ 20; Record at 21-40.

## II. Plaintiff's FOIA Request

On September 25, 2023, Plaintiff submitted a FOIA request to DOD seeking "a copy of the August 7, 2016 Fancy Bear/APT 28 Attribution Analysis provided by Manos Antonakakis and David Dagon referenced in the September 25, 2022 letter to Senator [Charles] Grassley." Whited Decl. ¶ 2. DOD acknowledged receipt of Plaintiff's FOIA request on September 26, 2023, and assigned the request record locator "23-F-1597." *Id.*

## III. This Litigation

Plaintiff initiated this lawsuit on November 20, 2023. *See generally* Compl., ECF No. 1. The complaint alleges violations of FOIA's disclosure obligations by three federal agencies: the National Archives and Records Administration ("NARA"), the U.S. Department of Homeland Security ("DHS"), and DOD. *Id.* ¶¶ 62-66. In the time since the complaint was filed, NARA and DHS have made interim and final productions responsive to Plaintiff's FOIA requests to those agencies. *See, e.g.*, Mar. 29, 2024 Joint Status report, ECF No. 22. Plaintiff later voluntarily dismissed his claims against NARA and DHS. Stipulated Order Dismissing Defendants NARA and DHS, ECF No. 52.

In response to Plaintiff's FOIA request to DOD, the agency searched for and located a 40-page report titled as Plaintiff had indicated in his request ("Fancy Bear/APT28 Attribution Analysis"). Whited Decl. ¶ 3. On March 21, 2024, DOD made a final response to Plaintiff's request. The cover email accompanying that response noted that DARPA was withholding the record in full under FOIA Exemption 3, which permits withholding of information whose disclosure is prohibited by statute, *see* 5 U.S.C. § 552(b)(3), because DARPA's initial review indicated that the record formed part of a technical proposal. Whited Decl. ¶ 4 & n.1. Although the cover email mentioned only Exemption 3 as a basis for withholding the record in full, the

record itself—which was attached to DOD's March 2024 response with each page redacted and applicable exemptions indicated in the upper-right corner of each page—shows that Exemption 4 was asserted over each page. *See generally* Record. The cover email also explained that DARPA had made underlying redactions under Exemptions 3, 6, 7(E), and 7(F). Whited Decl. ¶ 4.

Plaintiff responded by email to DOD's March 2024 final response, objecting to DOD's statement that the record formed part of a grant proposal. *Id.* ¶ 5. As a result, the agency agreed to reprocess the record. *Id.* DOD made its second final response on May 8, 2024. *Id.* The May 2024 response ceased to invoke Exemption 3, but continued to assert Exemption 4 over the entire record, and maintained underlying redactions under Exemptions 3, 6, 7(E), and 7(F). *Id.*

Plaintiff once again objected to DOD's renewed withholding-in-full of the record. *Id.* ¶ 6. DOD accordingly agreed once again to reprocess the record. *See id.* As required by Executive Order and DOD regulations, *id.* ¶¶ 5-6, the agency consulted with Georgia Tech about the appropriate scope of redactions under Exemption 4. After several rounds of consultation, Georgia Tech requested that DOD withhold more information under Exemption 4 than DOD believed to be justifiable on the basis of the rationales for withholding that the submitter had offered. *Id.* ¶ 6. In November 2024, DOD released the record to Plaintiff, with redactions made under Exemptions 3, 4, 6, and 7(E).[1] *Id.* At a subsequent status conference, Plaintiff indicated his intention to challenge all of the agency's redactions at summary judgment.

## LEGAL STANDARDS

FOIA was enacted to "pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny." *Dep't of Air Force v. Rose*, 425 U.S. 352, 361 (1976) (citation

[1] DOD will not defend its assertions of Exemption 3 at summary judgment. Because all of the information withheld under Exemption 3 is also redacted under other exemptions, it is not necessary to release a new version of the record to Plaintiff. Whited Decl. ¶ 8.

omitted). "Congress recognized," however, "that public disclosure is not always in the public interest," *CIA v. Sims*, 471 U.S. 159, 166-67 (1985), and "that legitimate governmental and private interests could be harmed by release of certain types of information." *FBI v. Abramson*, 456 U.S. 615, 621 (1982).

"Under the FOIA, each 'agency' upon 'any request' for records shall make the records 'promptly available to any person,' unless one of nine specific exemptions applies." *ACLU v. FBI*, 734 F.3d 460, 465 (6th Cir. 2013) (quoting 5 U.S.C. § 552(a)(3)(A) and then citing 5 U.S.C. § 552(b)(1)-(9)). Although FOIA's exceptions are to be "narrowly construed," *id.* (quoting *Akron Standard Div. of Eagle–Picher Indus., Inc. v. Donovan*, 780 F.2d 568, 571 (6th Cir. 1986)), they are nevertheless intended to have "meaningful reach and application." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151-52 (1989). An agency may withhold information under a FOIA exemption only if it "reasonably foresees that disclosure would harm an interest protected by an exemption" or if "disclosure is prohibited by law." 5 U.S.C. § 552(a)(8)(A)(i).

"Most FOIA cases are decided on summary judgment, since the primary question is a legal one: whether the withheld documents are covered by one of the statutory exemptions." *ACLU*, 734 F.3d at 465 (citing *Rimmer v. Holder*, 700 F.3d 246, 255 (6th Cir. 2012)). Summary judgment, in turn, is appropriately granted when the movant has established that "there is no genuine dispute as to any material fact," warranting "judgment as a matter of law." Fed. R. Civ. P. 56(a)). "[T]o facilitate review and the adversarial process, the government must support its position with detailed affidavits," which "are entitled to a "presumption of good faith." *ACLU*, 734 F.3d at 465 (quoting *Rugiero v. DOJ*, 257 F.3d 534, 544 (6th Cir. 2001)).

## ARGUMENT

The sole record at issue in this case—a 40-page report produced by a cyber-attack attribution laboratory at Georgia Tech and submitted to DARPA—contains extensive descriptions of the technology the laboratory used to analyze the 2016 "hack" of the Democratic National Committee's email servers. Those descriptions include closely held information regarding the statistical features the laboratory looks to in attributing cyber-attacks, as well as the data sources on which the algorithmic component of its technology relies. DOD has redacted both categories of that information. Those redactions were justified, as the covered information falls within the heartland of the "confidential commercial information" protected by Exemption 4, without which protection Georgia Tech would suffer economic harm. The Court can, and should, uphold the agency's redactions on this basis alone.

If the Court finds it necessary to look beyond DOD's well-founded assertions of Exemption 4, however, it should also uphold DOD's underlying redactions made under Exemptions 6 and 7(C) (to protect the privacy interests of third parties whose identifying information appears throughout the report) and Exemption 7(E) (to protect the techniques by which DARPA, through its research partners like Georgia Tech, attributes cyber-attacks and thus enforces the law).

### I. DOD Properly Withheld Confidential Commercial Information under Exemption 4

Exemption 4 to FOIA permits an agency to withhold "commercial or financial information obtained from a person and privileged or confidential."[2] The Whited Declaration establishes that the Exemption 4 redactions in this case were made to protect information that "is '(1) commercial or financial, (2) obtained from a person, and (3) privileged or confidential.'" *S. Envtl. L. Ctr. v.*

[2] Exemption 4 also permits the withholding of trade secrets, a category not at issue in this case. *See* 5 U.S.C. § 552(b)(4).

*Tenn. Valley Auth.*, 659 F. Supp. 3d 902, 912 (E.D. Tenn. 2023) (citing *Pub. Citizen Health Rsch. Grp. v. FDA*, 704 F.2d 1280, 1290 (D.C. Cir. 1983)). DOD is thus entitled to summary judgment as to its assertions of Exemption 4.

DOD redacted confidential commercial information that appears throughout the 40-page report at issue in this case. In particular, the information redacted identifies the sensitive statistical features of Georgia Tech's proprietary technology, as well as the data sources on which that technology relies to function. Whited Decl. ¶¶ 18, 20. Georgia Tech submitted the report to DARPA as an unpublished proof of concept in support of its anticipated participation in a DARPA research project aimed at developing and maintaining technology that can attribute cyber intrusions, or "hacks," to malicious online actors. *Id.* ¶ 11. The commercial entity to which Georgia Tech has licensed use of the university's technology is an established player in the world of cyber-attack attribution, *id.* ¶ 27, and relies on its proprietary algorithms and approach to attribution—referred to under the umbrella label of "attribution technology"—to remain competitive in receiving funding, *id.* ¶¶ 26-27. The laboratory thus jealously guards details of its attribution technology, as it did with respect to the report it submitted here. *Id.* ¶ 21.

Were the Exemption 4 redactions to be lifted, in turn, Georgia Tech would suffer commercial or financial harm. *Id.* ¶¶ 26-28. That is so because the information redacted, which falls into two categories (statistical features and data sources), would reveal centrally important (and confidential) aspects of the attribution technology to the outside. DOD has reasonably assessed that harm would befall Georgia Tech in either or both of two ways. First, would-be competitors to Georgia Tech's laboratory might reverse engineer the algorithm, depriving Georgia Tech of future business. *Id.* ¶ 25. And second, revelation of the sources on which Georgia Tech relies could lead malicious actors whose activities are revealed by the attribution technology to

spoliate or obfuscate those sources, reducing the value of Georgia Tech's product. *Id.* Exemption 4 exists to prevent precisely this type of harm, and so protects the information DOD has redacted here.

**a. The information withheld is commercial.**

The first element of a successful assertion of Exemption 4 over non-trade secret information is proof that the information withheld is "commercial." 5 U.S.C. § 552(b)(4). FOIA does not define the term, but "courts have 'consistently held'" that it "should be given [its] ordinary meaning." *Envtl. & Pol'y Inst. v. Tenn. Valley Auth.*, No.: 3:22-CV-220-TAV-DCP, 2024 WL 4535983, at *4 (E.D. Tenn. Oct. 21, 2024) (quoting *Pub. Citizen Health Rsch. Grp.*, 704 F.2d at 1290 (alteration in original)). The ordinary meaning of "commercial" "reaches . . . broadly," *Baker & Hostetler LLP v. U.S. Dep't of Comm.*, 473 F.3d 312, 319 (D.C. Cir. 2006), to include both information that is "commercial 'in and of itself'" and information in which the provider "has a commercial interest." *Citizens for Resp. & Ethics in Wash. v. DOJ*, 58 F.4th 1255, 1263 (D.C. Cir. 2023) ("*CREW*"). That "broad[]" definition, *Baker & Hostetler LLP*, 473 F.3d at 319, is consistent with the purpose of Exemption 4, which protects the interests of both the government and the submitter of the information by encouraging submitters to provide the government with accurate, reliable information and assuring submitters that such information will be safeguarded. *See, e.g.*, *Nat'l Parks & Conservation Ass'n v. Morton*, 498 F.2d 765, 767-70 (D.C. Cir. 1974), *abrogated on other grounds by Food Mktg. Inst. v. Argus Leader Media*, 588 U.S. 427 (2019) (concluding that the legislative history of FOIA "firmly supports an inference that [Exemption 4] is intended for the benefit of persons who supply information as well as the agencies which gather it"); *Critical Mass Energy Project v. Nuclear Regul. Comm'n*, 975 F.2d 871, 878 (D.C. Cir. 1992); *Bd. of Trade of City of Chi. v. CFTC*, 627 F.2d 392, 406 (D.C. Cir. 1980) (noting "the unmistakable

congressional purpose of avoiding impairment of the Government's ability to obtain necessary information"), *abrogated on other grounds by U.S. Dep't of State v. Wash. Post Co.*, 456 U.S. 595 (1982).

The statistical features of Georgia Tech's algorithmic technology, and the data sources on which that technology relies, are intrinsically commercial because they "serve[] a commercial function [and are] of a commercial nature," *CREW*, 58 F.4th at 1263 (quoting *Nat'l Ass'n of Home Builders v. Norton*, 309 F.3d 26, 38 (D.C. Cir. 2002)). The Whited Declaration explains that the statistical features of the technology that have been redacted reveal the way the technology works. Whited Decl. ¶¶ 18, 25. That information "serves a commercial function" in that it encapsulates precisely what is commercially valuable about the product. So too for the data sources, without which the product would not be commercially valuable. *Id.* ¶¶ 18, 25. The statistical features and data sources are "of a commercial nature" for the same reasons.

The redacted information concerning statistical features and data sources is also commercial because Georgia Tech maintains a commercial interest in it, and particularly in its continued nondisclosure. *See CREW*, 58 F.4th at 1263, 1265 (noting a company's commercial interest in "data or reports on its commercial service or its product's favorable or unfavorable attributes." (quoting *Baker & Hostetler LLP*, 473 F.3d at 319)); *see also Varnum LLP v. U.S. Dep't of Lab.*, No. 1:18-cv-1156, 2021 WL 1387773, at *4 (W.D. Mich. Mar. 15, 2021) ("Customer information is commercial and/or financial information because BCBSM has a commercial interest in this information." (citations omitted)); *cf. Seife v. U.S. Food & Drug Admin.*, 43 F.4th 231, 240 (2d Cir. 2022) ("[Exemption 4] therefore contemplates harm specifically to commercial or financial interests."). The statistical features of the technology and the data sources it relies on are, in essence, the "ingredients" that make the technology successful. Whited Decl. ¶ 18; *cf.*

*Herrick v. Garvey*, 298 F.3d 1184, 1190 (10th Cir. 2002) ("We have defined a 'trade secret' for the purposes of FOIA as 'a secret, commercially valuable plan, formula, process, or device that is used for the making, preparing, compounding, or processing of trade commodities and that can be said to be the end product of either innovation or substantial effort.'" (citation omitted)). If the statistical features of the technology are revealed, competitor entities will be put in a position to reverse engineer Georgia Tech's product. Whited Decl. ¶ 25. Alternatively, the value of the product itself may be destroyed if the sources on which the technology relies to function (indeed, without which it cannot function) are compromised. *Id.* That risk is not merely hypothetical. As the circumstances under which this report was produced evince, attribution of cyber-attacks to malicious online actors (including foreign actors) is a priority of the United States government. *Id.* ¶ 17. Those actors, in turn, have an interest in evading detection, and will all but certainly take steps to do so if they can. *Id.* ¶ 28.

The aforementioned features of the information withheld under Exemption 4 places it squarely within the category of information that courts have routinely held to be commercial. *See, e.g.*, *Leopold v. U.S. Dep't of Just.*, No. 19-cv-3192 (RC), 2021 WL 124489, at *6 (D.D.C. Jan. 13, 2021) (report containing "extensive proprietary, financial, and competitive business information about HSBC and its customers" was commercial); *Naumes v. Dep't of Army*, 588 F. Supp. 3d 23, 37 (D.D.C. 2022) ("[T]he materials satisfy the first prong[, commercial nature,] inasmuch as routine release of copyrighted information through FOIA requests would undermine the market for the creator's work in much the same way that the release of other types of commercial information could inflict competitive harm."); *100Reporters LLC v. U.S. Dep't of Just.*, 248 F. Supp. 3d 115, 136 (D.D.C. 2017) ("probing reviews of . . . business systems and practices," descriptions and evaluations of "compliance programs, including references to finance functions,

mergers and acquisitions practices, and sales and marketing," details of "country operations, projects, contracts, and bids" all commercial); *Waterkeeper All. v. U.S. Coast Guard*, No. 13-cv-0289, 2014 WL 5351410, at *15 (D.D.C. Sept. 29, 2014) (information related to "oil and gas leases, prices, quantities and reserves" was commercial).

Georgia Tech's status as a public research institution does not undercut the conclusion that the information its laboratory submitted is commercial. *See Smolen v. FAA*, No. 22-cv-44, 2023 WL 3818105, at *6 (S.D.N.Y. June 2, 2023) ("[A]n association need not generate taxable profits for its information be 'commercial or financial.' There is no qualifier that the association or organization be for profit or generate taxable income; public organizations, for example, frequently do not generate taxable income. It is sufficient that it be an association and that the character of the information pertains to commerce. Non-profit organizations as well, just like public or private organizations, engage in commerce and have commercial and financial information which is protected by FOIA Exemption 4." (citations omitted)).

In this respect, the information at issue here is materially distinct from that which the D.C. Circuit determined was not commercial in *Washington Research Project, Inc. v. Department of Health, Education and Welfare*, 504 F.2d 238 (D.C. Cir. 1974). There, the court held that biomedical researchers' research designs submitted in conjunction with projects funded by the National Institute of Mental Health were not "commercial" because the scientists who submitted them were not "engaged in trade or commerce." *Id.* at 244. Instead, those researchers had an interest in "professional recognition and reward." *Id.* at 245. Here, in contrast, the Whited Declaration shows that Georgia Tech has commercialized the technology at issue and profits from its licensing. Whited Decl. ¶¶ 23-24. Whatever the character of Georgia Tech as an institution or

its nonprofit mission more generally might be, its commercial information (particularly where licensed for consideration, *id.* ¶ 24) falls within the protection of Exemption 4.

**b. DOD obtained the information withheld from "a person."**

The second required element for withholding under Exemption 4 is that the confidential, commercial information be obtained "from a person." 5 U.S.C. § 552(b)(4). In turn, FOIA defines "person" to include "an individual, partnership, corporation, association, or public or private organization other than an agency." *Id.* § 551(2). This requirement serves primarily to distinguish between information obtained from other government agencies and information obtained from without government. *See Ctr. for Auto Safety v. U.S. Dep't of Treasury*, 133 F. Supp. 3d 109, 119 (D.D.C. 2015). Georgia Tech is a "public or private organization," *see* 5 U.S.C. § 551(2), and so meets this requirement.

**c. The information withheld is confidential.**

Finally, non-trade secret information must be "confidential" to be withheld under Exemption 4. *See Argus Leader Media*, 588 U.S. at 433-34 (quoting 5 U.S.C. § 552(b)(4)). In *Argus Leader Media*, the Supreme Court interpreted "confidential" to mean, consistent with its ordinary usage, "private" or "secret." *Id.* at 433-34. And one essential element of information that is confidential, the Supreme Court reasoned, is that it be "customarily kept private, or at least closely held, by the person imparting it." *Id.* at 434.

As a general matter, Georgia Tech keeps private the statistical features and data sources that were redacted in the record. Whited Decl. ¶ 21. And with respect to this record in particular, Georgia Tech explicitly requested that the agency not divulge its contents. *Id.*; *see also* Record at 2 n.1. Were more needed, the Whited Declaration confirms that the circumstances under which

this report ordinarily include the expectation that submission to the grantor agency will not destroy the commercial value of the technology used to produce the report. Whited Decl. ¶ 21.

In *Argus Leader Media*, the Supreme Court also identified a second potential component of confidentiality: that the "party receiving it provides some assurance that it will remain secret." 588 U.S. at 434. It was unnecessary in that case to resolve whether this second facet of confidentiality is an essential one for information to be deemed confidential under Exemption 4. *Id.* at 434-35. So too in this case, as the requirement (to the extent it is a requirement) is met here. The Whited Declaration confirms that the circumstances under which the government received the report—direct submission from a private party to its government funder—is one in which the agency customarily guarantees confidentiality. Whited Decl. ¶ 21. That is particularly the case for the sensitive research that DARPA undertakes. *Id.* The information Georgia Tech submitted to DARPA thus meets the confidentiality requirement of Exemption 4. *See Am. Small Bus. League v. U.S. Dep't of Def.*, 411 F. Supp. 3d 824, 832-33 (N.D. Cal. 2019).

**d. The agency reasonably foresees harm to protected interests from disclosure.**

To qualify for withholding under FOIA, information must not only satisfy the requirements specific to the statute's listed exemptions—the withholding agency must also demonstrate that (for all exemptions save Exemption 3) it reasonably foresees disclosure "harm[ing] an interest protected by an exemption." 5 U.S.C. § 552(a)(8)(A)(i)(I); *see Seife*, 43 F.4th at 235 (describing the foreseeable-harm requirement).

DOD has adequately established that reasonably foreseeable harm will follow if the statistical features and data sources presently redacted in the report are publicly disclosed. Indeed, the agency's anticipated harms overlap to a significant extent with the same rationales under which Georgia Tech has a commercial interest in the redacted information. Part I.a, *supra*. The agency's

predicted harms take two forms. First, if the statistical features of Georgia Tech's technology are revealed, the university will suffer competitive harm in the limited, highly competitive market of cyber-attack attribution because its competitors will be enabled to reverse engineer their product, which is unique. Whited Decl. ¶¶ 25-26. That reverse engineering will, in turn, decrease the commercial value of Georgia Tech's product. Second, revelation of the data sources on which the technology relies will likely lead to those data sources being spoiled (rendered useless) or manipulated to decrease their utility as part of a cyber-attack attribution software. *Id.* ¶ 25. This, too, will lead to a diminution in the commercial value of Georgia Tech's product.

## II. DOD Properly Withheld Personal Information under Exemptions 6 and 7(C)

Because all of the redactions DOD made under Exemptions 6, 7(C), and 7(E) fall within redactions made under Exemption 4, the Court need not address these latter exemptions unless it disagrees with Defendant that summary judgment on its Exemption 4 redactions is proper. In any event, those redactions, too, are justified.

DOD has properly redacted personally identifiable information under Exemptions 6 and 7(C).[3] Both of these exemptions safeguard personal privacy interests. Exemption 6 protects information about individuals in "personnel and medical files and similar files." 5 U.S.C. § 552(b)(6), *see Wash. Post Co.*, 456 U.S. at 600-02 (interpreting Exemption 6's use of "similar files" to have a "broad meaning," including "detailed Government records on an individual which

[3] Defendant asserts Exemption 7(C), on a basis coextensive with its Exemption 6 redactions, for the first time in these district court proceedings. Under FOIA, an agency does not waive an argument that an exemption applies by not raising it during the administrative process. *See Maydak v. DOJ*, 218 F.3d 760, 764 (D.C. Cir. 2000) ("[A]s a general rule, [the government] must assert all exemptions at the same time, in the original district court proceedings."); *Shapiro v. DOJ*, 153 F. Supp. 3d 253, 269 n.6 (D.D.C. 2016) ("Although the FBI did not rely on its categorical policies in denying Truthout's request at the administrative level, the D.C. Circuit has long implied that an agency may invoke a FOIA exemption for the first time before the district court—but not 'for the first time in the appellate court.'" (quotation omitted)).

can be identified as applying to that individual"); *Cizek v. Dep't of Def.*, 2024 WL 4332111, at *8 (D.D.C. Sept. 27, 2024) ("The purpose of Exemption 6 is 'to protect individuals from the injury and embarrassment that can result from the unnecessary disclosure of personal information.'" (quoting *Wash. Post Co.*, 456 U.S. at 599)). 7(C), in turn, covers "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C); *see DOJ v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 762 (1989) (construing "privacy interest" to include "avoiding disclosure of personal matters").

To invoke either exemption, an agency must balance the privacy interest implicated against the public interest purportedly justifying disclosure. *Dep't of Def. v. FLRA*, 510 U.S. 487, 497 (1994) (Exemption 6 balancing); *Reporters Comm.*, 489 U.S. at 776 (Exemption 7(C) balancing). But the weight of the respective interests in the balancing equation differs as between the two provisions: Exemption 7(C), which applies only to "records or information compiled for law enforcement purposes," 5 U.S.C. § 552(b)(7), forbids disclosure where it could "reasonably be expected" to result in an "unwarranted" invasion of personal privacy. *Id.* § 552(b)(7)(C). Exemption 6, in contrast, poses a higher bar for withholding information, requiring a "clearly unwarranted invasion of personal privacy." *Id.* § 552(b)(6); *see Reporters Comm.*, 489 U.S. at 756.

**a. The record was compiled for law-enforcement purposes.**

At the threshold of any invocation of Exemption 7, an agency must establish that it "compiled" the record in question "for law enforcement purposes." 5 U.S.C. § 552(b)(7). That is true of DOD's acquisition of the record Plaintiff sought and obtained.

To start, DOD (through its subcomponent, DARPA) "compiled" the record when it obtained it from Georgia Tech. It is immaterial that Georgia Tech is not itself a law-enforcement agency. *See John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 153 (1989). What matters is instead that the government have compiled (*i.e.*, "composed," "collected," or "assembled," *id.*) the record in question for the purpose of law enforcement by the time it invokes Exemption 7. *Id.*; *see also id.* ("This definition seems readily to cover documents already collected by the Government originally for non-law-enforcement purposes." (citation omitted)). DARPA did so here. A research component of DOD, DARPA was executing a law-enforcement mission in gathering data useful for identifying (potentially illegal) cyber intrusions. Whited Decl. ¶ 31; *see McMichael v. Dep't of Def.*, 910 F. Supp. 2d 47, 52 (D.D.C. 2012) ("A record is compiled for law enforcement purposes when it "focus[es] directly on specifically alleged illegal acts, illegal acts of particular identified officials, acts which could, if proved, result in civil or criminal sanctions." (alteration in original) (quoting *Rural Hous. All. v. Dep't of Agric.*, 498 F.2d 73, 81 (D.C. Cir.1974)); Indictment, ECF No. 1, *United States v. Netyksho*, No. 1:18-cr-215 (D.D.C. July 13, 2018) (announcing criminal charges against foreign individuals in connection with a cyber-attack).

**b. Individuals whose information appears in the record have a privacy interest in nondisclosure.**

Throughout the report, DOD has redacted information pertaining to third parties. That information includes internet protocol ("IP") addresses, email addresses, names (including names that appear within email addresses), and photos. Whited Decl. ¶ 32. Disclosure of that information would plainly infringe on the privacy interests of those individuals, who have (to Defendant's knowledge) not explicitly consented to disclosure, *id.* ¶ 34, because it would enable them to be identified in connection with a government record with which they otherwise have not personally volunteered a connection. *See Sutton v. IRS*, No. 05 C 7177, 2007 WL 30547, at *6 (N.D. Ill. Jan.

4, 2007) (upholding redactions of personal information relating to "third-party taxpayers"); *Fritz v. IRS*, 862 F. Supp. 234, 236 (W.D. Wis. 1994) (protecting name and address of person who purchased requester's seized car); *see also Broward Bulldog v. U.S. Dep't of Just.*, 939 F.3d 1164, 1184 (11th Cir. 2019) (describing "names, addresses, and phone numbers" as personal details triggering 7(C)); *Maryland v. U.S. Dep't of Vets.' Affs.*, 130 F. Supp. 3d 342, 353 (D.D.C. 2015) (same, for email addresses); *Advoc. for Hwy. & Auto Safety v. Fed. Hwy. Admin.*, 818 F. Supp. 2d 122, 128-29 (D.D.C. 2011) (videotaped images triggered privacy interest). DOD thus generally applies a policy of withholding personal information like that redacted here to avoid "annoyance, threats, or harassment in their private lives," as it has done here. Whited Decl. ¶¶ 29-30.

**c. There is no cognizable public interest in disclosure.**

On the other side of the scales, the identified privacy interest must be weighed against the public's interest in disclosure. But crucially, not any generic "public" interest qualifies. Rather, "the only relevant 'public interest in disclosure' to be weighed in this balance is the extent to which disclosure would serve the 'core purpose of the FOIA,' which is 'contributing significantly to public understanding of the operations or activities of the government.'" *FLRA*, 510 U.S. at 495 (analyzing Exemption 6) (quoting *Reporters Comm.*, 489 U.S. at 775) (alteration omitted); *see also Detroit Free Press v. DOJ*, 829 F.3d 478, 485 (6th Cir. 2016) (applying this logic in the 7(C) context). The requestor bears the burden to establish the existence of a cognizable public interest. *NARA v. Favish*, 541 U.S. 157, 172 (2004) (Exemption 7(C) "requires the person requesting the information to establish a sufficient reason for the disclosure"); *Associated Press v. DOJ*, 549 F.3d 62, 66 (2d Cir. 2008) (describing this burden in terms applicable to Exemptions 6 and 7(C) alike). The identity of the requestor, and her reasons for seeking the information, are irrelevant. *Reporters Comm.*, 489 U.S. at 771. Instead, the appropriate inquiry is into "the nature of the requested

document and its relationship to 'the basic purpose of the Freedom of Information Act.'" *Id.* at 772 (quoting *Rose*, 425 U.S. at 372). Moreover, the requestor "must not only present an interest that is both public and significant, but also demonstrate that disclosure of the information sought will further that interest." *Rimmer*, 700 F.3d at 258.

Plaintiff has not proffered a public interest to justify overcoming the individuals' privacy interest in nondisclosure, but it is doubtful he could do so. Indeed, revealing the personally identifying information of individuals connected to sources on which Georgia Tech relied in producing a research product would not, in any conceivable way, demonstrate "what the government is up to." *See Fitzgibbon*, 911 F.2d at 768 (quoting *Reporters Comm.*, 489 U.S. at 772-73). Because there is no cognizable public interest in disclosure, Plaintiff necessarily cannot "demonstrate that disclosure of the information sought will further that interest." *Rimmer*, 700 F.3d at 258. And, absent a public interest, the Court "need not linger over the balance." *Beck v. DOJ*, 997 F.2d 1489, 1494 (D.C. Cir. 1993) (quotation omitted). After all, "something outweighs nothing every time," *id.* (alteration and quotation omitted), whether under the Exemption 6 or 7(C) criteria for conducting that balancing. *See, e.g.*, *Detroit Free Press*, 829 F.3d at 484-85 (engaging in 7(C) balancing).

**d. Foreseeable harm would result from the disclosure of information redacted under Exemptions 6 and 7(C).**

As under Exemption 4, DOD must demonstrate that disclosure of the information it has redacted under Exemptions 6 and 7(C) would cause foreseeable harm prevented by those exemptions. *See* 5 U.S.C. § 552(a)(8)(A)(i)(I). The agency has done so here. The requisite connection is straightforward: the individuals whose privacy interests are implicated by their personally identifiable information in the record would have those interests inherently infringed if their private information were exposed to the public. *Reporters Comm.*, 489 U.S. at 763

(describing the privacy interests protected by FOIA as encompassing "the individual's control of information concerning his or her person"); *Am. First Legal Found. v. U.S. Dep't of Homeland Sec.*, No. 21-cv-2168, --- F. Supp. 3d ----, 2024 WL 4932041, at 13 (D.D.C. Dec. 2, 2024). Were more needed, the Whited Declaration identifies follow-on harms that the agency has reasonably determined will follow from disclosure: "annoyance, threats, or harassment in their private lives." Whited Decl. ¶¶ 30, 33. This personal information was thus properly withheld under Exemptions 6 and 7(C).

## III. DOD Properly Withheld Information Regarding Law-Enforcement Techniques Under Exemption 7(E)

Finally, DOD properly made certain underlying redactions pursuant to Exemption 7(E) to protect "techniques . . . for law enforcement investigations" that "could reasonably be expected to risk circumvention of the law." *See* 5 U.S.C. § 552(b)(7)(E). As described above, the report—which was authored by a U.S. government research partner—analyzes in detail a cyber-attack believed to have been perpetrated by a foreign adversary of the United States. DARPA relies in part on the analyses of its partners to carry out its law enforcement mission of identifying such malicious actors. Accordingly, albeit indirectly, certain features of Georgia Tech's analysis are properly classified "techniques" of the agency that are subject to redaction under Exemption 7(E).

### a. The record was compiled for law-enforcement purposes.

As for redactions made under Exemption 7(C), successful invocation of Exemption 7(E) requires at the threshold that the record in question have been compiled for a law enforcement purpose. For the reasons given at Part II.a, *supra*, the record at issue here qualifies.

**b. Disclosure of the information redacted would reveal DARPA's law-enforcement techniques.**

A "technique" within the meaning of Exemption 7(E) is "a technical method of accomplishing a desired aim." *Allard K. Lowenstein Int'l Hum. Rts. Proj. v. DHS*, 626 F.3d 678, 682 (2d Cir. 2010) (quoting Webster's Third International Dictionary). DARPA has identified one of its desired aims as ascertaining which online actors are responsible for particular cyber-attacks. Whited Decl. ¶ 17. That aim, in turn, forms part of the agency's general law-enforcement mission. *Id.* ¶ 31. And in addition to the research DARPA conducts itself, it funds research through partners like Georgia Tech as one technique to carry out that mission of cyber-attack attribution. *Id.* ¶ 38.

Under Exemption 7(E), DARPA has protected "specific state-of-the-art techniques to identify bad cyber actors," *id.*, by hiding "datasets, location operations, and other sources used to investigate United States adversaries," *id.* Much as Georgia Tech's analysis provides a roadmap to DARPA to identify the authors of cyber-attacks, revealing these features of the technology (and data sources on which it relies) would provide adversaries a roadmap of sorts to the features that the United States government finds relevant in its efforts to do the same. The information redacted would therefore reveal "techniques . . . for law enforcement investigations" if disclosed. *See* 5 U.S.C. § 552(b)(7)(E); *Families for Freedom v. U.S. Customs & Border Prot.*, 837 F. Supp. 287, 296-97 (S.D.N.Y. 2011) (agency properly withheld under 7(E) information "address[ing] how often the Border Patrol checks various specific trains, what time of day and at what stations it makes those checks, how its agents board and navigate the trains, and other issues relating to the agency's law enforcement techniques").

**c. Disclosure of the information redacted would lead to reasonably foreseeable harm.**

Much like the disclosure of the information redacted under Exemption 4 would lead to commercial harm to Georgia Tech, exposing the same information also redacted under Exemption 7(E) would harm DARPA's law-enforcement mission. DARPA relies on tools like the one Georgia Tech has developed and licensed to identify actors who, the agency knows, seek to evade detection. Whited Decl. ¶¶ 28, 38. If the bases for the agency's detection were to be made public, those actors would be put on notice in a way that would enable their evasion, undercutting the agency's ability to detect them (and, by extension, the ability of other agencies to interdict them). Because DOD has demonstrated a link between the foreseeable harm it anticipates would arise and the disclosure of information subject to Exemption 7(E), its redactions were proper.

## IV. DOD Has Released All Reasonably Segregable, Non-Exempt Information

Where portions of an agency record are exempt from disclosure under FOIA, the agency must examine the remainder of the record to determine which information, if any, is releasable without causing harm against with the statute's exemptions protect. *Leopold v. Dep't of Just.*, 94 F.4th 33, 37 (D.C. Cir. 2024) (quoting 5 U.S.C. § 552(a)(8)(A)(ii), (b)). In assessing an agency's compliance with FOIA's segregability requirement, "[a]ffidavits attesting to the agency's 'line-by-line review of each document[]' and the agency's determination 'that no documents contained releasable information which could be reasonably segregated from the nonreleasable portions,' in conjunction with a *Vaughn* index describing the withheld record, suffice." *Ecological Rts. Found. v. U.S. Envtl. Prot. Agency*, 541 F. Supp. 3d 34, 66 (D.D.C. 2021) (quoting *Johnson v. Exec. Off. for U.S. Att'ys*, 310 F.3d 771, 776 (D.C. Cir. 2002)).

DOD has carried that burden here. To start, the Whited Declaration attests that the agency reviewed the report line by line to determine which information was exempt from disclosure and

which was releasable. Whited Decl. ¶ 39. Indeed, the record itself shows the care and precision with which the agency approached its task: redactions are made throughout, often on a word-by-word basis. *See generally* Record. While a *Vaughn* index per se is not necessary here, because only one record is at issue, the Whited Declaration comprehensively details the type of information redacted and where it appears in the document. *See generally* Whited Decl.; *see also Schoenman v. FBI*, 604 F. Supp. 2d 174, 196 (D.D.C. 2009) (describing the contents of a *Vaughn* index).

**CONCLUSION**

For the foregoing reasons, Defendant respectfully requests that the Court grant its motion for summary judgment and enter judgment in its favor.

Dated: February 28, 2025

Respectfully submitted,

YAAKOV M. ROTH
Acting Assistant Attorney General
Civil Division

ELIZABETH J. SHAPIRO
Deputy Director
Federal Programs Branch

*/s/ Simon Gregory Jerome*
SIMON G. JEROME
D.C. Bar No. 1779245
Trial Attorney
United States Department of Justice
Civil Division
Federal Programs Branch
1100 L St., N.W.
Washington, D.C. 20005
(202) 514-2705
simon.g.jerome@usdoj.gov

*Counsel for Defendant*